Version

Serial Number

Signature Algorithm ID

Issuer Name

Validity Period

Subject Name

Subject Public Key Info

Signature (by CA)

Prior Art

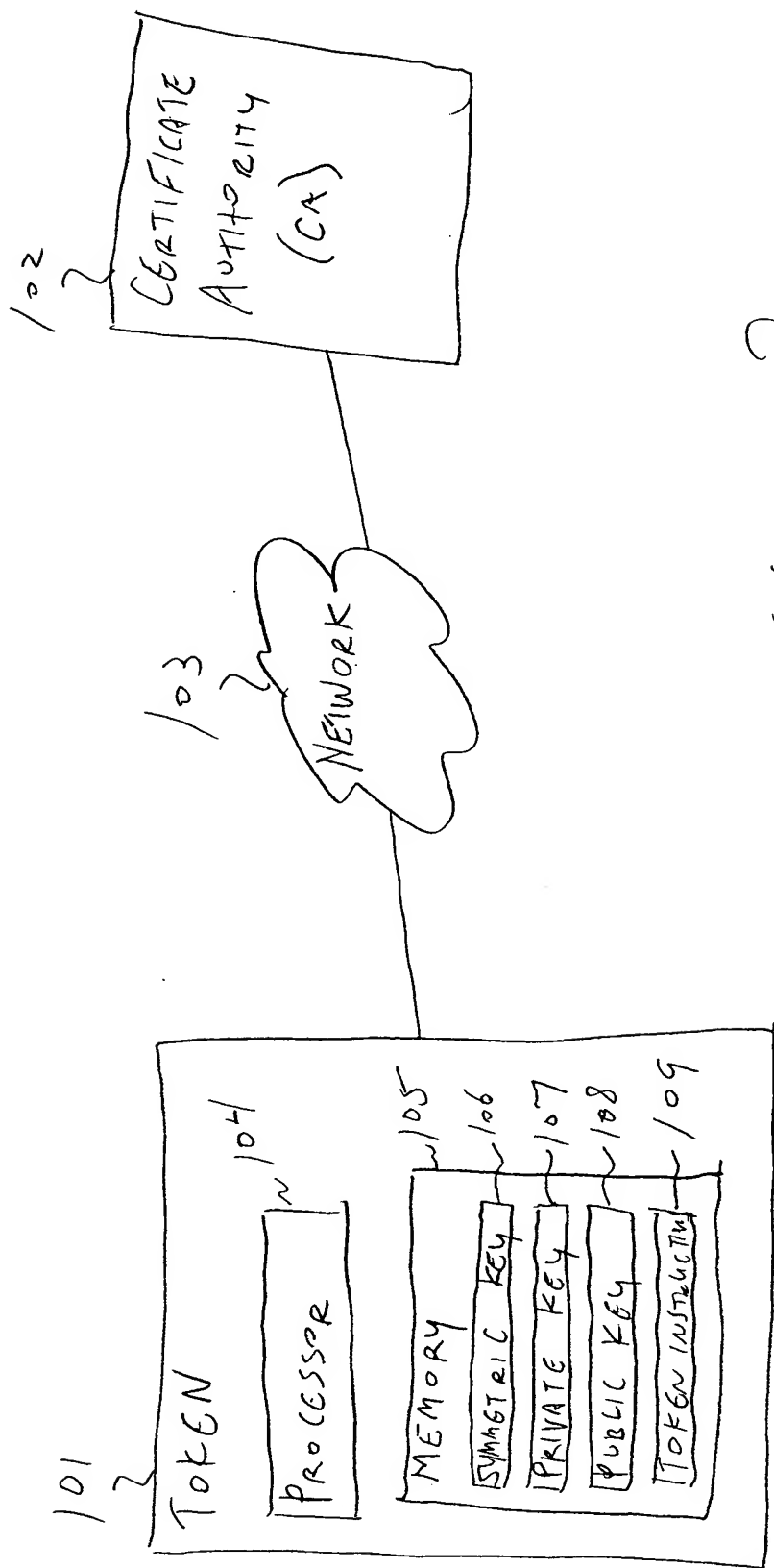Figure 1
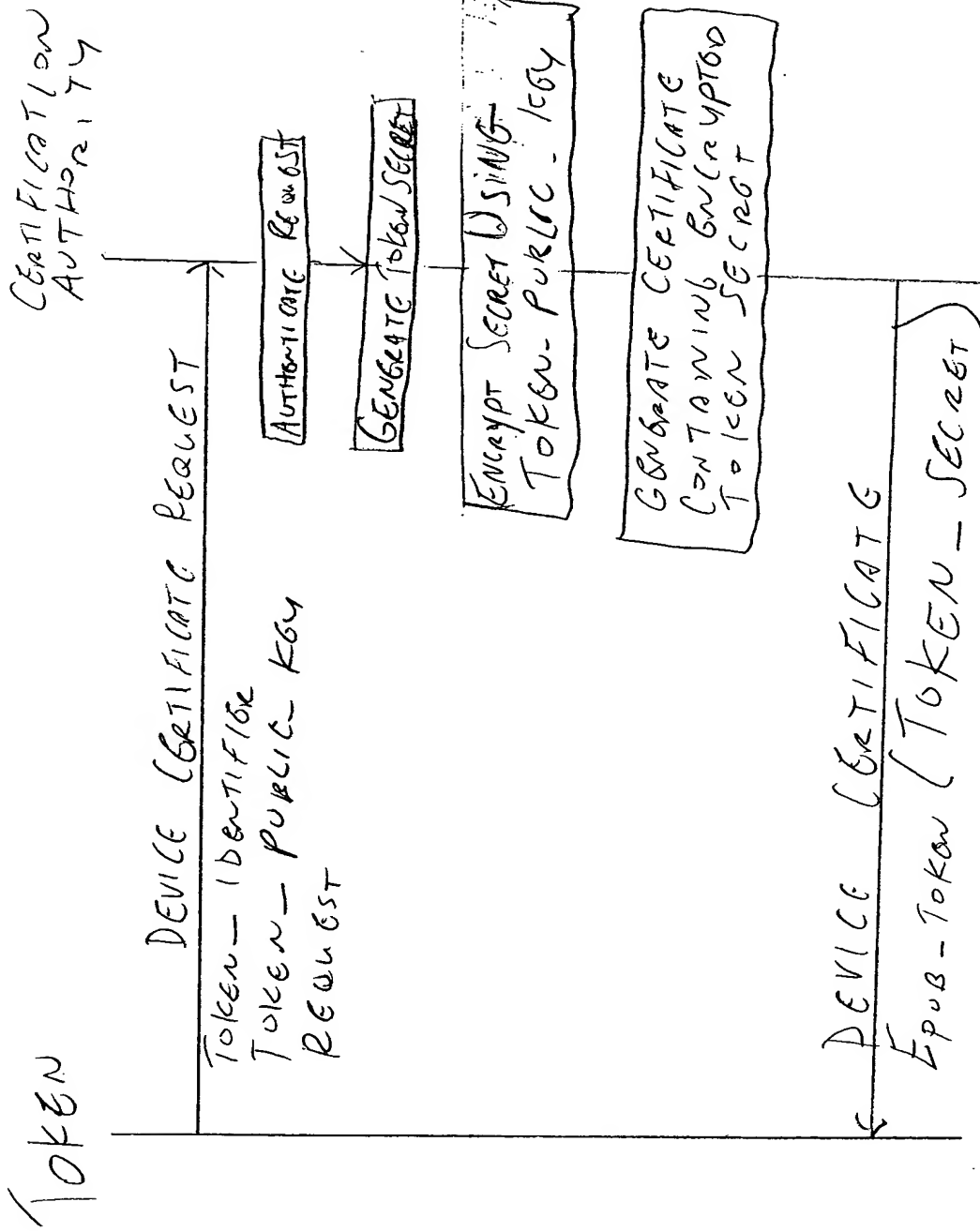
CERTIFICATE
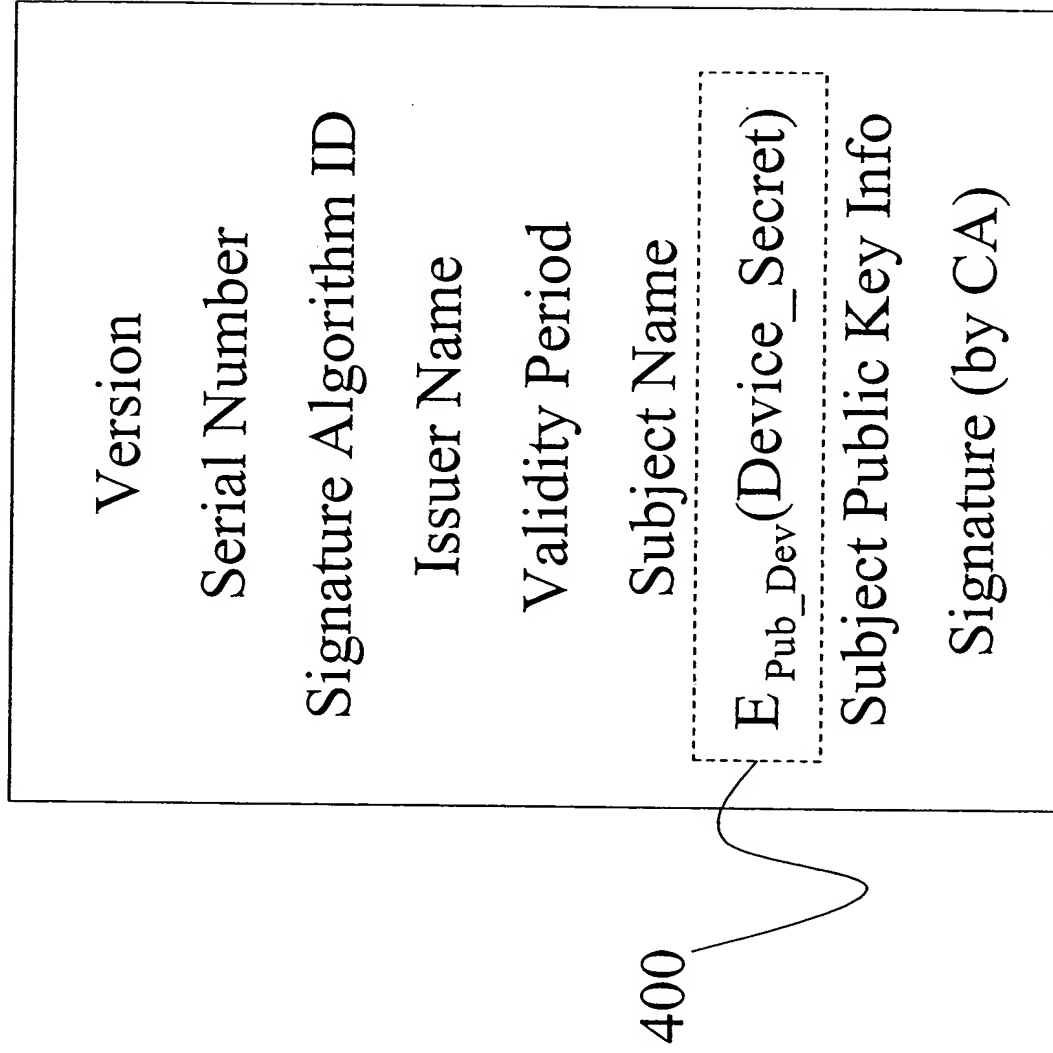AUTHORITY
(CA) 102

NETWORK 103

TOKEN 101

PROCESSOR 104

MEMORY 105
SYMMETRIC KEY 106
PRIVATE KEY 107
PUBLIC KEY 108
TOKEN INSTRUCTION 109

FIGURE 2

Token

Certification Authority

Device Certificate Request

Token_Identifier
Token_Public_Key
Request

Authenticate Request

Generate Token Secret

Encrypt Secret Using Token_Public_Key

Generate Certificate Containing Encrypted Token Secret

Device Certificate (Token_Secret)

$E_{Pub-Token}$ (Token_Secret)

FIGURE 3

Version

Serial Number

Signature Algorithm ID

Issuer Name

Validity Period

Subject Name

$E_{Pub\_Dev}(Device\_Secret)$

Subject Public Key Info

Signature (by CA)

400

Figure 4